AOP 9: COMPUTER OPERATIONS SECURITY

9.1 BACKGROUND

The purpose of this document is to establish an AOP for the control and safeguarding of the computing environment of the DFS.

9.2 REFERENCES

9.2.1 Code of Virginia (COV); Article 7.1 (' '18.2-152.1 to 18.2-152.15) “Virginia Computer Crimes Act”.

9.2.2 COV ITRM Standard 90-1 Information Technology Security.

9.2.3 COV ITRM Standard SEC2001-01.1.

9.2.4 Code of Virginia ' '19.2-310.5 and 19.2-310.6.

9.2.5 Quality Manual & 13.13, Records Security.

9.3 POLICY

9.3.1 DFS will ensure the security, confidentially and integrity of all of its data programs and the information stored therein. These programs include but are not limited to the Forensic Automated Case Tracking System (F.A.C.T.S.), Combined DNA Index System (CODIS), Automated Fingerprint Identification System (AFIS), DNA Databank, Breath Alcohol DataBase & National Integrated Ballistics Information Network (NIBIN).

9.3.2 Acceptable use of DFS computer resources, bulletin boards, on-line subscriptions and the Internet consists of activities that conform to the purpose, goals and mission of the Division of Forensic Science and each user’s authorized job functions.

9.4 INFORMATION SECURITY

9.4.1 Logon ID’s and passwords will be used to authenticate user access to all DFS Computer Systems. The computer system will require the user to change passwords every 30 days. The computer system will maintain a history of user passwords to ensure a unique password is used for a period of 24 months.

9.4.2 All users should log-off or lock the program/computer when leaving the computer so unauthorized users will not have access to it. To further improve the security of all programs the computer system will automatically lock the computer after 10 minutes of none activity (the user must use his/her password to unlock the computer). All computers (except those whose continued operation is required) will be turned off (powered-down) at close of business.

9.4.3 Critical computer applications and data, residing on designated servers/directories, will be backed up daily (except weekends). At least one complete backup tape per week will be stored off site.

9.5 PHYSICAL SECURITY

9.5.1 It is the responsibility of each member of the staff to protect the computer equipment, data and applications/programs. Computers, software and storage media are to be used for Division authorized purposes only and will not be removed from Division premises without permission.

9.5.2 System Configuration

9.5.2.1 The configuration of the Division's Computers is maximized to meet the requirements for a program or programs used on the various computers. .

9.5.2.2 Configuring a PC entails such things as ensuring that there is a sufficient amount of RAM available to load all the necessary programs that are required as well as specifying the sequence of the loading of the various programs and drivers. Optimal configurations have been developed for the computers at the expense of a great deal of time and effort. The division will not permit "customization" of the configurations of the computers, except for those computers dedicated to specific instrumentation. Consequently, system administrators are the only personnel authorized to make changes to PC configurations. This prohibition does not extend to the customizing of colors, button bars, etc., which may be part of authorized applications or the graphical user interface – (Microsoft Windows Desktop).

9.6 COMPUTER VIRUSES

9.6.1 The major source of computer viruses comes from email and the use of software acquired from outside sources. To preclude the introduction of a virus into any division system, the following acts are prohibited:

9.6.1.1 The use of bootlegged software or software of unknown or questionable origin.

9.6.1.2 The unauthorized use of applications acquired from public networks.

9.6.2 In addition to being subject to disciplinary action under the Standards of Conduct for violating these prohibitions, an employee may also be responsible for any expenses incurred by the Division as a result of the introduction of a computer virus into the Division's computer environments.

9.6.3 From time to time, software is available from other forensic laboratory systems or from public networks for use or evaluation. To ensure such media is free of viruses, it should be checked before being introduced onto any of the Division's systems. To expedite and isolate this examination, each PC connected to the DFS network will have anti-virus software loaded on it. While no virus protection program can protect against all viruses, these programs will guard against most of the more prevalent ones. Periodically updating the virus program will ensure that it is current. All questionable software must be checked in this manner.

9.7 SOFTWARE COPYRIGHT

9.7.1 It is the policy of the DFS to abide by copyrights and purchase the necessary software in the desired number of copies directly from authorized vendors. Software piracy will not be condoned. Each PC requiring a copy of the software will have one legally licensed copy of the appropriate software or a company-authorized permit to install it. It is the responsibility of the Laboratory Directors and their system administrators to ensure that copyright requirements are met for computers under their control.

9.7.2 If a staff member violates this copyright policy and the Division must make payment to a vendor as a result of such violation, the employee, in addition to being subject to disciplinary action under Standards of Conduct, may be required to reimburse the Division for such payment plus any expenses incident thereto.

9.8 AUTHORIZED SOFTWARE

9.8.1 It is the policy of DFS that only authorized software will be installed and used on its computers.

9.8.2 Authorized software is defined as software purchased by the Division or software from other sources that is authorized by the Division.

9.8.2.1 To receive approval to use an individual's personal software on a state computer, to acquire and use software from public networks (shareware), or to use software provided by other laboratory systems, the requestor must make a written request that includes the following:

- Name of user
- Name of software package and source
- Intended use of the software package
- PC on which the software package will be loaded
- For personal software, a copy of the license agreement pertaining to the software package
- For shareware, the cost, if any, of the registration fee and to whom it is to be paid

9.8.2.2 The request will be forwarded through the local system administrator to the Director of the laboratory in which the software will be used. The Laboratory Director will forward the request to the Deputy Director together with a recommendation.

9.8.2.3 Once approval is given, actual installation will be contingent upon the software successfully completing a virus check with the laboratory's virus checker.

9.8.3 Purchase requests for software (including shareware but excluding CODIS, NIBIN, AFIS, etc.), accompanied by a written justification, will be forwarded to the local system administrator who will make a recommendation to the Director of the laboratory. If the Laboratory Director recommends approval, the request will follow normal purchasing channels.

9.9 POLICY VIOLATIONS

9.9.1 Maintenance of the security, confidentiality and integrity of the Division's computer systems is a very serious business and requires constant diligence on everyone's part. A breech of this AOP is a very serious matter and will be dealt with accordingly under the Standards of Conduct.

◆ End